UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,382	12/21/2001	Michael A. Epstein	US010632	4889

24737 7590 07/07/2006

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,382	EPSTEIN, MICHAEL A.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-6 have been considered. After careful and thorough consideration, Examiner maintains the position presented in the previous action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Akiyama, European Patent Application No. EP 1,041,767.

As per claims 1 and 4, the applicant describes a hashing system with the following limitation which is met by Akiyama:

a) a plurality of hash devices ([0029]);

b) each hash device of the plurality of hash devices being configured to receive a sequence of data values and apply a hash function to the received subset of the sequence of data values when enabled, said hash function being the same in said each hash device ([0029], [0050], Fig 1, Fig 3A);

c) at least one comparator, operably coupled to the plurality of hash devices, that is configured to compare an output of each hash device to the source hash value, to facilitate a verification of the sequence of data values ([0030], Fig 1).

As per claims 2 and 5, the applicant describes the hashing system of claims 1 and 4, which are met by Akiyama, with the following limitation which is also met by Akiyama:

Wherein each hash device is enabled sequentially ([0062], Fig 4B).

As per claims 3 and 6, the applicant describes the hashing system of claims 1 and 4, which are met by Akiyama, with the following limitations which are also met by Akiyama:

a) said each hash device is enabled to receive and process K data values (Fig 4A, Fig 4B);

b) the plurality of hash devices corresponds to K hash devices (Fig 4A, Fig 4B).

Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent No. 5,907,619.

As per claims 1 and 4, the applicant describes a hashing system with the following limitation which is met by Davis:

a) a plurality of hash devices (Col 5, lines 21-28; Fig 3);

b) each hash device of the plurality of hash devices being configured to receive a sequence of data values and apply a hash function to the received subset of the sequence of data values when enabled, said hash function being the same in said each hash device (Col 5, lines 21-28; Fig 3);

c) at least one comparator, operably coupled to the plurality of hash devices, that is configured to compare an output of each hash device to the source hash value, to facilitate a verification of the sequence of data values (Col 5, lines 21-28; Fig 3).

As per claims 2 and 5, the applicant describes the hashing system of claims 1 and 4, which are met by Davis, with the following limitation which is also met by Davis:

Wherein each hash device is enabled sequentially (Col 5, lines 21-28; Fig 3).

As per claims 3 and 6, the applicant describes the hashing system of claims 1 and 4, which are met by Davis, with the following limitations which are also met by Davis:

a) said each hash device is enabled to receive and process K data values (Col 5, lines 21-28; Fig 3);

b) the plurality of hash devices corresponds to K hash devices (Col 5, lines 21-28; Fig 3).

Response to Arguments

Applicant's arguments, see Remarks filed 6/16/06, with respect to the 112 second paragraph rejection of claim 1 have been fully considered and are persuasive. The 112 second paragraph rejection of claim 1 has been withdrawn.

Applicant's arguments with respect to the 102(b) rejection of claim 1 under Akiyama have been fully considered but they are not persuasive. Applicant presents the following argument:

1) Akiyama does not teach that the hash function is the same

Examiner respectfully disagrees. To begin with, Examiner notes that this argument was previously presented (see Remarks 10/6/05). Examiner's instant response is the same as that given in the previous action (mailed 2/16/06). More specifically, Applicant has argued that "Akiyama teaches applying different hashing functions-- using different keys K1, K2, ... Kn-- to the data blocks D1,D2 ...Dn" (see Remarks 10/6/05, page 1). Applicant further submitted paragraph [0014].

Having fully and carefully considered Akiyama, Examiner respectfully disagrees that Akiyama teaches use of more than one hashing function. The language of Akiyama seems to suggest that more than one hashing algorithm is employed. Citing the paragraph submitted by Applicant, Akiyama discloses the following: "A signing station executes a step of preparing a plurality of authenticators by applying a different one-way function to each data" [0014].

However, a closer look into Akiyama reveals that what is meant by the above is that a different key is employed while the hashing function, itself, remains the same. Fig 3A illustrates the hashing system disclosed by Akiyama, wherein each hashing unit (2 of Fig 3A) relies on the same hash function (22 of Fig 3A). Well-known hashing functions include MD5, SHA-1, etc. The hashing units employ different keys (K1,K2,K3) on input data (D1,D2,D3) and thus produce different authenticators

(CS1,CS2,CS3). However, the hashing function-- be it MD5, SHA-1, etc-- is the same in each hash device.

A goal of the Akiyama reference is to employ different keys on the same hashing algorithm. By so doing, it becomes difficult for a third party to forge an authenticator, because in addition to knowing such factors as the hashing function and the data, a third party must also know the different keys [0034]. To restate, well-known hashing functions include MD5, SHA-1, etc. NOTHING in the Akiyama reference teaches that one hashing function (such as MD5) is used in one hash computation while a distinct hashing function (such as SHA-1) is used in another hash computation. While such an odd and unconventional practice could potentially be pragmatic in that a third party must also know the different hashing functions, as well as the different keys, as well as which hashing functions are used with which keys, such a practice is simply not disclosed by Akiyama.

In contrast, Akiyama teaches that a single one-way function, though perhaps keyed by a different key, is applied in each hash computation. Fig 2A shows a specific configuration of a hash system and illustrates three hash computations, employing one one-way function designated by 22. When describing Fig 3A, another illustration of the hash system, Akiyama further clarifies that one one-way hash function is employed: "Fig 3A shows configuration of a case where n in Fig 2A is set to 3. The same reference numerals as those in Fig 2A are assigned to the hash units 2, the EOR21, **the one-way function 22**, and the truncator, and detailed description thereof is omitted herein" [0050] (emphasis added).

In his latest Remarks, Applicant refers to paragraph [0025] and argues that the hash units have different one-way functions (see Remarks page 2, lines 5-7). Examiner cites paragraph [0025] in its entirety:

> "The **hash units 2 have one-way functions for converting data D1 to Dn using keys K1 to Kn** to authentication signs CS1 to CSn respectively, and they output the converted authentication signs CS1 to CSn to the linking unit 5. Although it is assumed that **the hash units 2 perform processing corresponding to a known hash function** in a protocol or the like for a method of verifying authentication signs based on the conventional technology, it is not always required that reverse conversion is ensured" [0025].

Examiner respectfully submits that nothing in the paragraph above is inconsistent with Examiner's foregoing remarks. Examiner reiterates that what is meant by "one-way functions" is that a different key is employed while the hashing function, itself, remains the same. Thus, Akiyama teaches "hash units 2 hav[ing] one-way functions...using keys K1 to Kn" (first sentence of [0025]). Further, Akiyama, in the very next sentence, states that "the hash units 2 perform processing corresponding to **a** known hash function" (second sentence of [0025]). There is nothing in this paragraph or anything in the remainder of Akiyama to suggest that in addition to employing different keys, the units employ separate hash algorithms, such as known algorithms MD5, SHA-1, etc.

Applicant further argues that teaching of different hash algorithms "is further supported by the need for a different key (K1 to Kn) for each function 22" (Remarks, page 2 lines 17-18). Examiner respectfully, but most strenuously, disagrees with the foregoing. A "need for a different key" (if one exists in the reference?) lends nothing to the argument that different hash algorithms are employed. Different keys are utilized in the reference so as to make it extremely difficult for a third party to forge the authenticator [0034], since a third party would need to have all the different keys to create a forgery.

For at least the reasons given above, Examiner maintains the rejections.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER